HowTo

# Avira AntiVir Server

## Support

March 2010

www.avira.com

Content

This document helps you to install and configure Avira AntiVir Server in an optimal way. It contains important and helpful settings and recommendations of the Avira Support for the configuration of the program. Furthermore you find useful hints e.g. the procedure in case of a virus attack.
You find all installation files and product manuals in pdf format on our website:

http://www.avira.de/en/download/index.html

## 1. Setup Modes

After having downloaded the installation file of Avira AntiVir Server, start the setup file “avira_antivir_server_en.exe”.

If you download the zip package, extract the files to a separate directory, navigate to the directory “en-us” and start “setup.exe”.

Now the assistant appears. Please, click on next. You have the possibility to choose the setup type:

### 1.1 Complete:

AntiVir Server is installed completely with the service Avira AntiVir Server and the console AntiVir Server Consoles. You can’t choose a target folder for the program files.

### 1.2 Custom:

You can decide if you want to install the service Avira AntiVir Server and/or the AntiVir Server Console.
You can install the AntiVir Server Console on a workstation in order to be able to access on remote the server service.

**Hint:**
Installation of the service  Avira AntiVir Server: If you want to access the protected server on remote with the AntiVir Server Console, make sure that the following ports are opened:

139 (NetBIOS SSN)
137 (NetBIOS NS)
138 (NetBIOS DGM)

You can choose a target folder for the program files which have to be installed.

After that the dialogue window “Install license” appears. Choose the directory where you have saved the license file (hbedv.key). You can also test the Avira AntiVir Server for 30 days.

Afterwards the installation is started.

It is possible that the installation of the Microsoft Visual C++ 2008 is also started in case the kit wasn't installed before.

**Hint:**

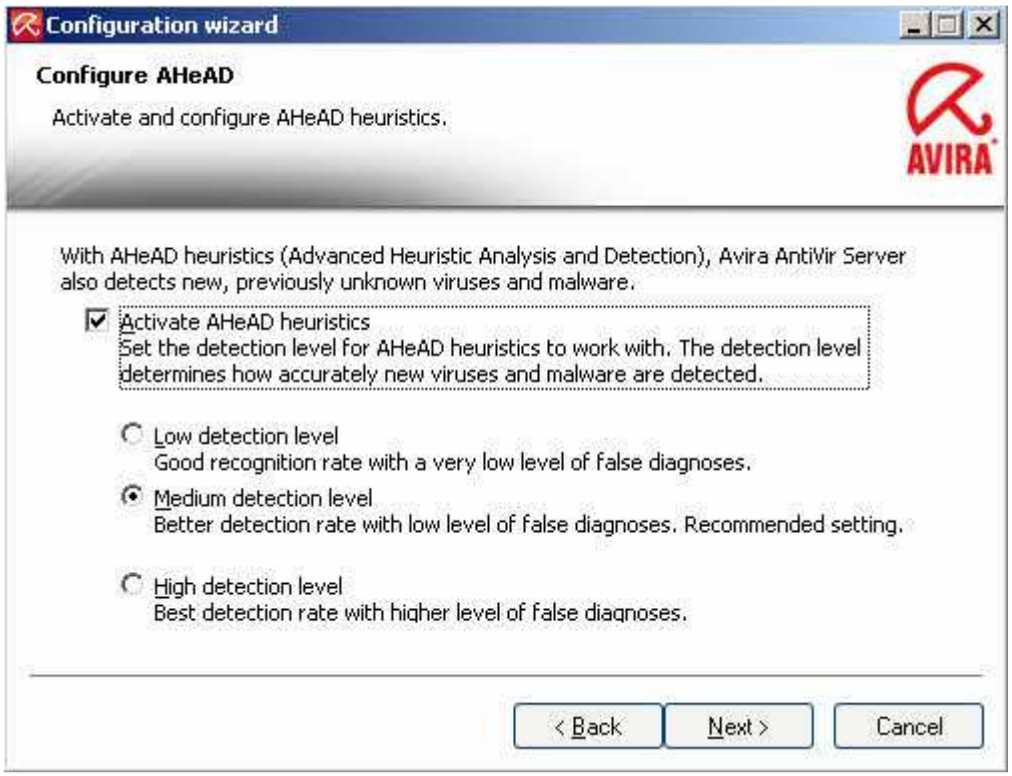
Avira AntiVir Server uses runtime libraries of the Micorsoft Visual C++ 2008 – redistributable kit. The installation of Microsoft Visual C++ 2008 - redistributable kit is required for the usage of Avira AntiVir Server.

The link for the downlad of the redistributable kit is:

http://www.microsoft.com/downloads/details.aspx?FamilyID=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=de

As soon as you have finished the installation the configuration assistant appears. The assistant guides you through the basic settings of the Avira AntiVir Server.

In the following dialogue window you can configure the engine and the detection level of the AHeAD technology. The chosen detection level is applied to the settings of the AHeAD technology of the scanner (direct scan) and the Guard (on access scan).

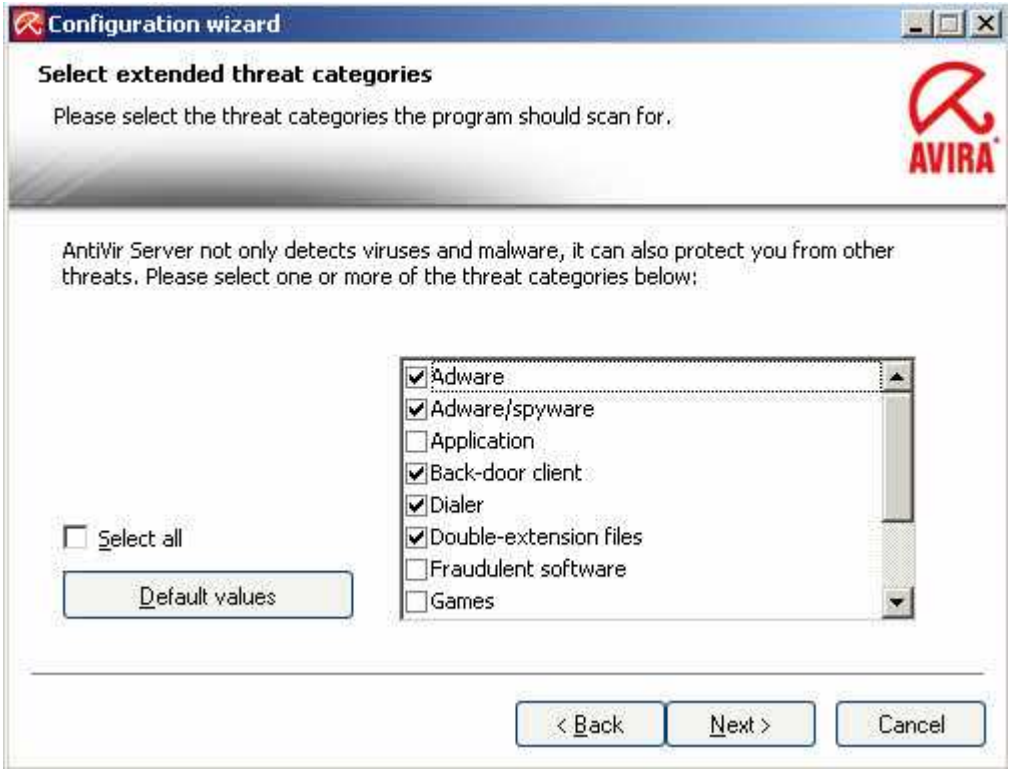



**Please, be aware that a high detection level detects a large quantity of unknown malware, but it also increases the risk of false positives.**

*What does heuristic mean?*

Heuristic is a method of detection which is able to detect unknown viruses. A profound analysis of the code looks for functions which are typical for viruses. In case the examined code has suspicious characteristics, AntiVir indicates the suspicious file. This doesn't mean that the code is really a virus, false positives are possible.

In the following dialogue window you can choose the extended threat categories.

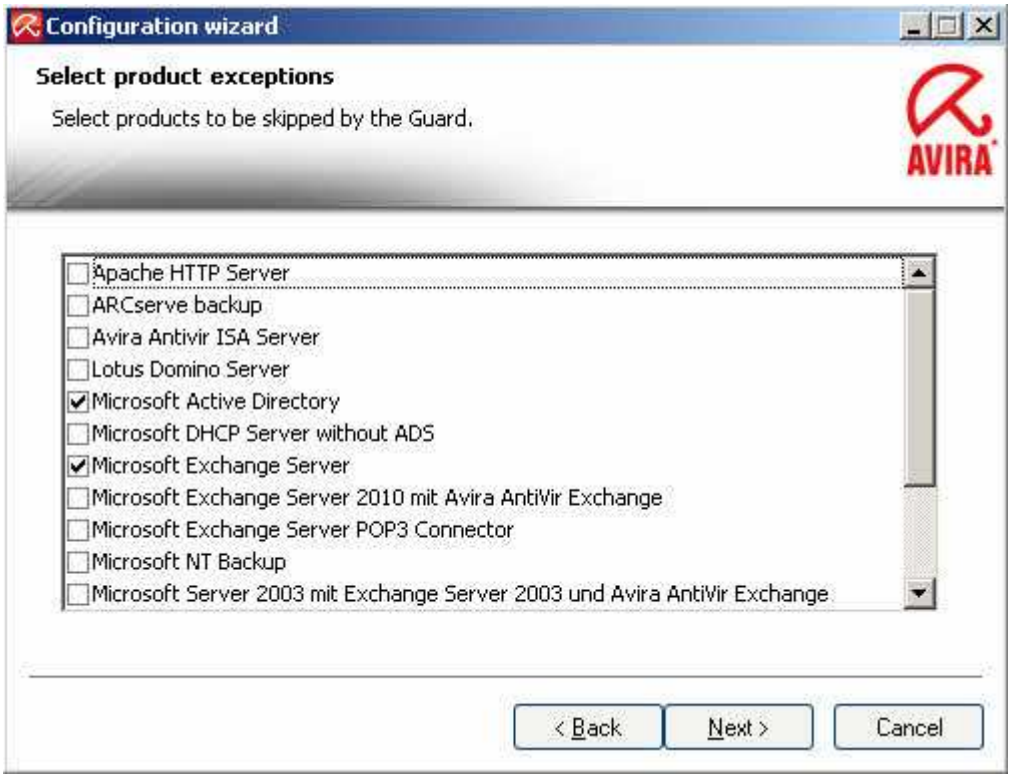



These options are activated by default as the risks of adware/spyware and back-door control software, phishing and dialers are very high. However, many administrator tools are detected by Avira as "Security Privacy Risk". AntiVir cannot distinguish if a suspicious program is used intentionally by an admin. This is why we excluded application, SPR and games from the default settings.

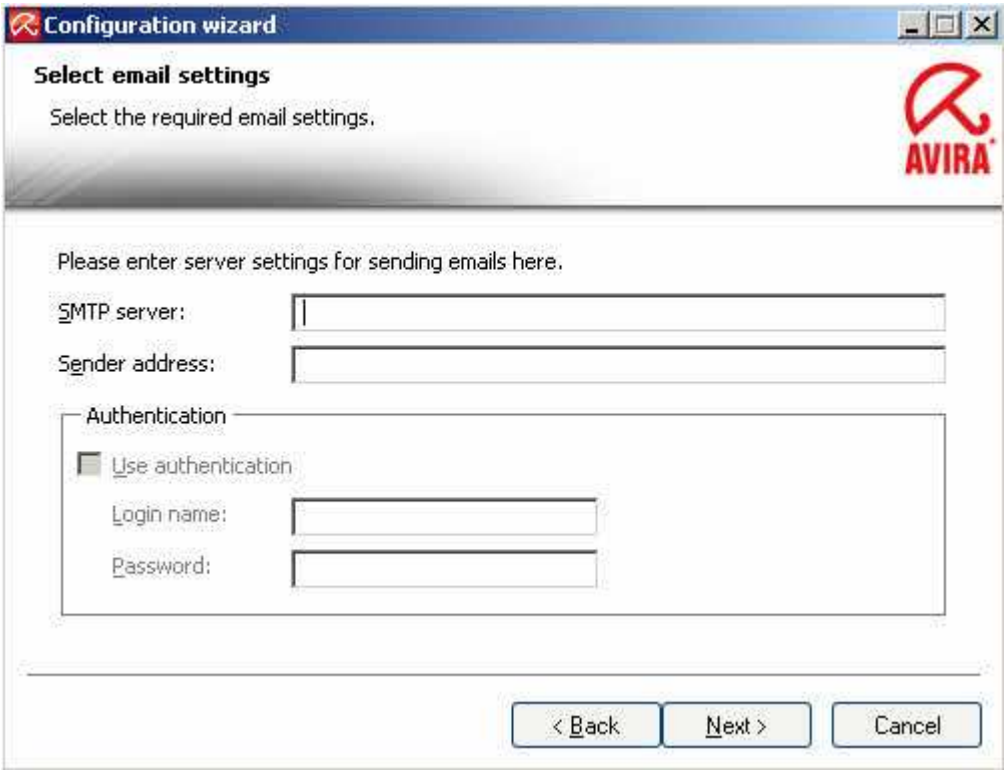
You can find an overview of all threat categories and their meaning in the quick tips at the end of this document.

Please, choose afterwards the products which you want to exclude from the supervision of the Guard (on access scanner). Thus you can avoid losses of performance and side effects which can be caused by the Guard.

Most programs are already predefined by Avira. In case you should use one of these programs, please exclude it from the scan by marking it.




In the next configuration dialogue you can choose the settings for the email notifications. AntiVir Server uses emails via SMTP for the sending of warnings of the different modules Guard, Scanner and Updater.
In case you don't know the data of your SMTP server or you don't want to use this option you can leave these boxes empty.



# 2. Configuration

## 2.1 Update configuration for the Internet Update Manager

In case you want to use several installations of AntiVir Server or AntiVir Professional in your network and update them centrally you can do that by means of the free module “Internet Update Manager”.
This is very helpful in case only one computer should have access to the internet but you want to update the virus definition files on all your computers in the network. Furthermore you limit the traffic and don’t load the internet connections unnecessarily.

You find the necessary tool in the following link:

http://www.avira.de/en/downloads/avira_antivir_server.html

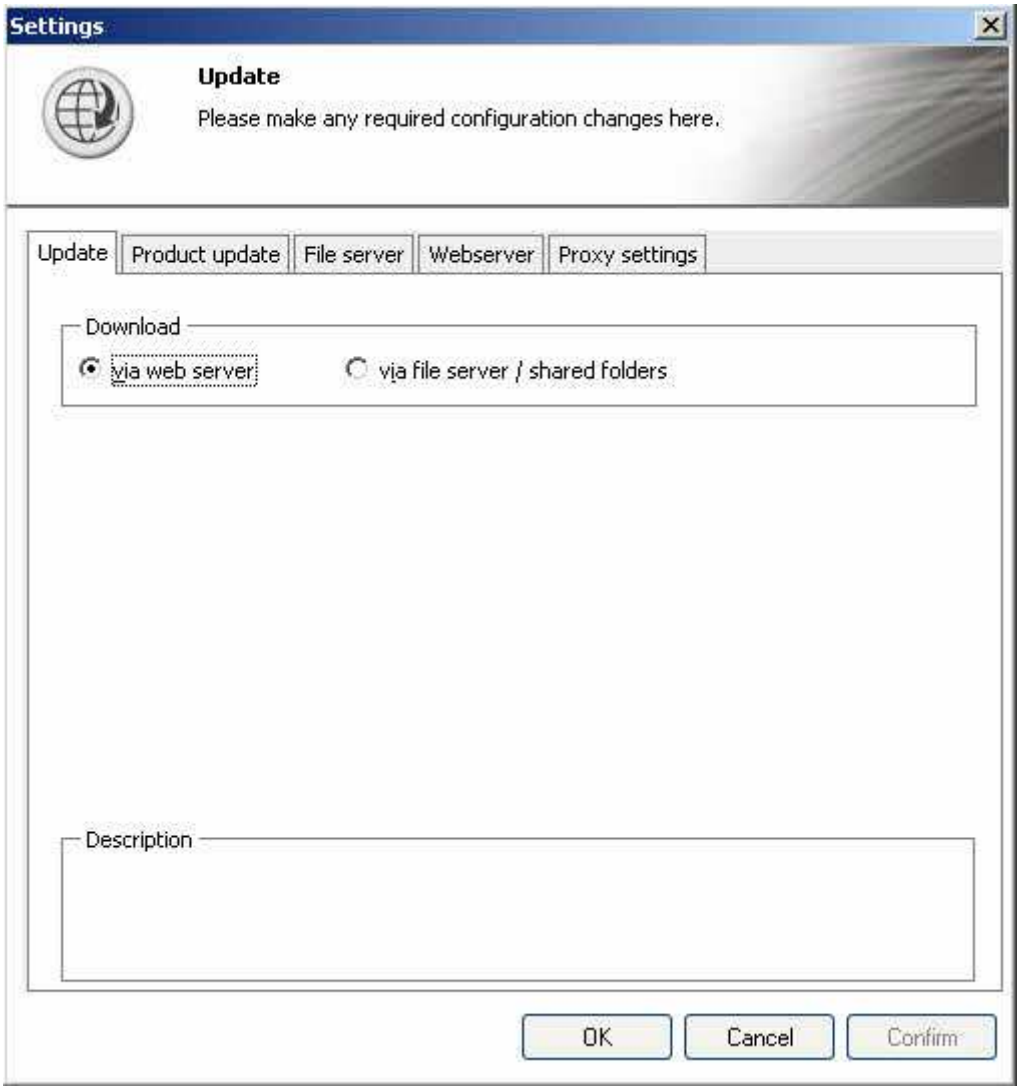
You can install this software on a usual workstation or on a server. In case of an installation on a workstation, keep in mind that only 10 network connections are possible at one time. You find detailed information about the installation and configuration of the Internet Update Manager in the corresponding manual, which you find on the following link:

http://www.avira.de/en/downloads/avira_antivir_server.html

After the installation of the Internet Update Manager and the configuration, the virus definition files of the Avira AntiVir Server are downloaded at the scheduled intervals and saved into the root directory.
As the Internet Update Manager provides an integrated web server with the port 7080, all workstation in the local network can connect to this directory and load their updates there.

In order to configure the Avira AntiVir Server, please, proceed as follows:

Open the configuration of the Avira AntiVir Server.
Go to the menu point “Settings” and “Update”. Choose “Download” and the option “Via web server”.




Afterwards go to the point “Webserver”. Here you have two boxes, “Priority server” and “Default server”.

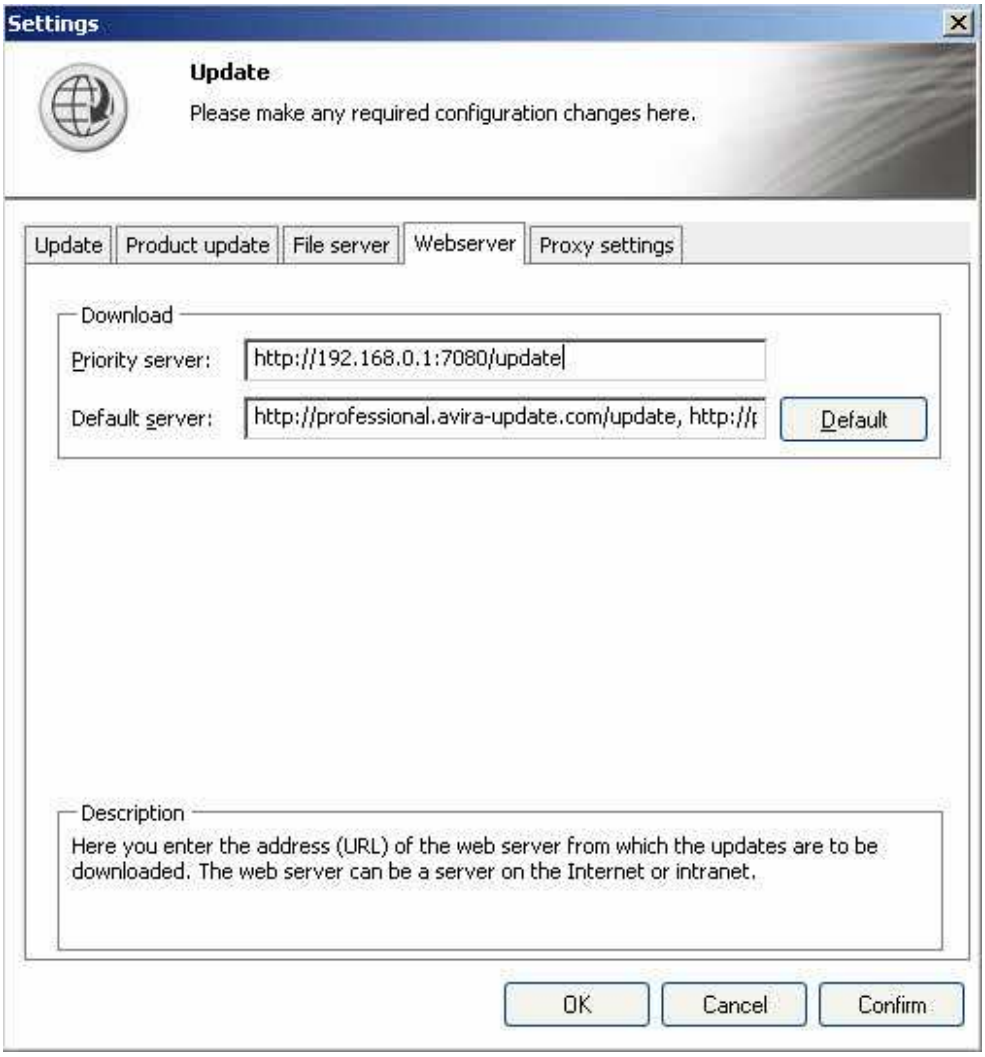
Avira AntiVir Server tries to contact the priority server in the first place. In case there is no connection to the priority server available, AntiVir tries to get a connection to the default server.
Therefore the function “Priority server” should be used for the updates via the Internet Update Manager (IUM). This is very useful if notebooks are used in the enterprise network which have to be updated also being outside the network.

In case the IUM computer is offline, the Avira AntiVir Server contacts the default server automatically if you have configured the priority server (IUM address) and the default server (Avira download server).

The following information should be entered into this box:

http://[IP-Adresse des IUM-Rechners]:7080/update (AntiVir 9 and 10)
http://[IP-Adresse des IUM-Rechners]:7080/upd (AntiVir 8)

Example:
http://192.168.0.1:7080/update
http://192.168.0.1:7080/upd




You can change the port of the Internet Update Manager if this port is already occupied in your network. Double click the navigation menu of the Internet Update Manager on the corresponding server (default setting: “local host”) → “settings” → “Networks”. Here you can change the port of the server from 7080 to the required port.

Accordingly, the settings for the update configuration of the Avira AntiVir Professional have to be changed.

It is important that the chosen path is enabled in the whole network and in each firewall of the workstations.

## 2.2 Configuration of product updates

You find the point “Product updates” in the configuration settings of the update of Avira AntiVir Server. Avira provides you with updates of the software in irregular intervals in order to correct program malfunctions or to offer new functions.
If you set automatic program updates here, keep in mind that a server **reboot** might be necessary. The reboot is initiated automatically by AntiVir Server.

You avoid this enforced reboot by choosing the notification in case of product updates. You configure that via the menu of AntiVir Server “Settings” → “Update” and the options in the menu point “Product updates”.

Afterwards you can schedule when the product updates should be installed, e.g. in a time period when the server can be rebooted without causing any inconveniences.

## 2.3 Setting exceptions

Avira AntiVir Professional is connected directly to the operating system. Especially the Avira AntiVir Guard scans all files during the real-time scan at each write or read access. It is therefore recommended to exclude special programs and their processes from the AntiVir scan.

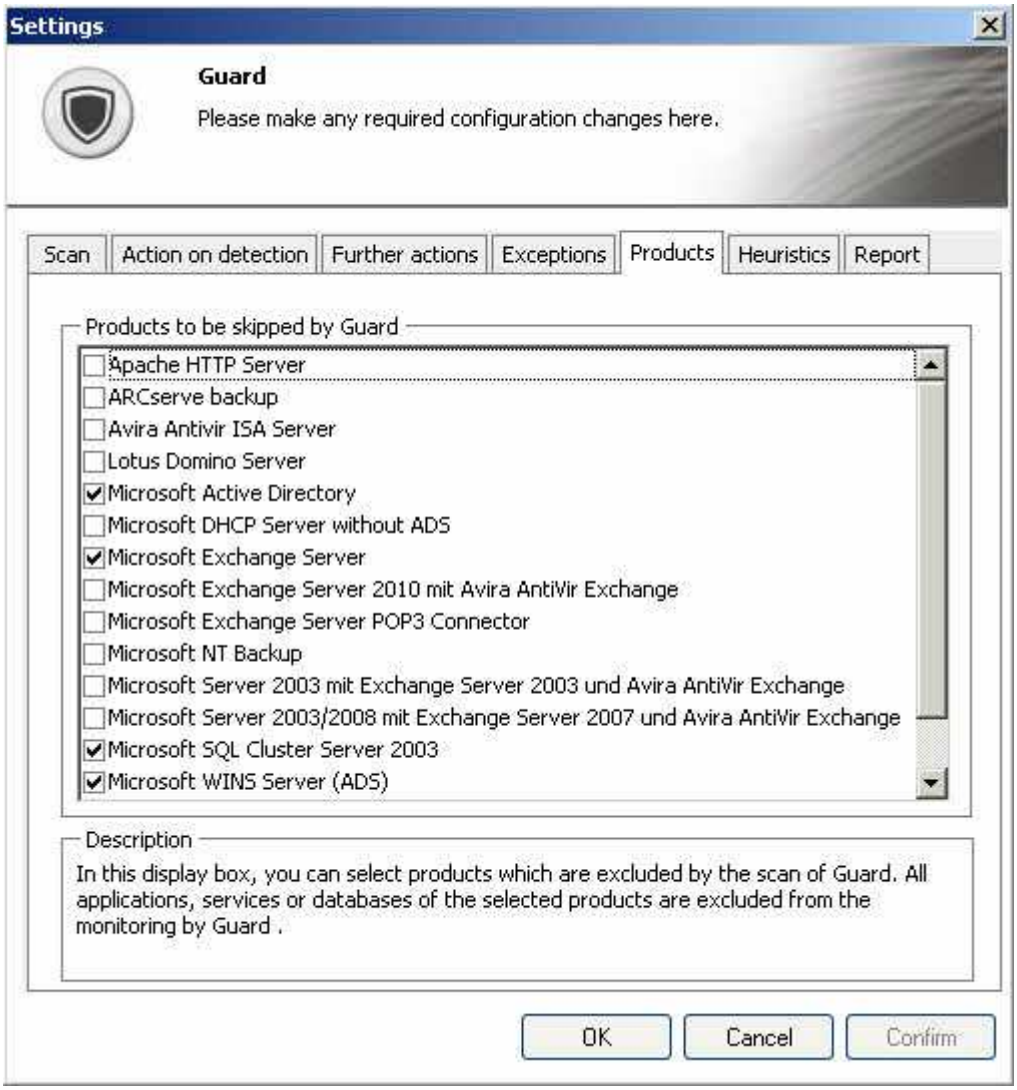
For example all programs which operate with a database in the background are concerned like accounting programs, financial software, mail server or web server.

Furthermore special backup programs which require a data backup of your systems are concerned. During a backup a read access is made of all files of the computer and the guard constantly scans each file which is saved by the backup program. This can affect the performance of your computer.

In order to prevent a slowing down of your system and exclude the concerning programs from the scan, please, proceed as follows:

- Start the configuration of Avira AntiVir Server
- Go to the menu “Settings”
- Open the point “Guard”
- Choose here the point “Products”

In the menu „products“ you find the programs which are already predefined by Avira. These programs can cause a loss of performance if they are not excluded from the scan. In case you should use one of these programs, please, exclude it from the scan by marking it.




In case you should use a special backup software or another software working with a data base which is not contained in this list, please, go to the point “exceptions”.
In the menu “Processes to be skipped by Guard” you have to enter the paths of the program folders where the concerned software is installed. It is important that the entered path is followed directly with a “\” so that AntiVir recognizes the path as a directory and not as a file.

An example for a correct path entry: C:\ProgramXY\

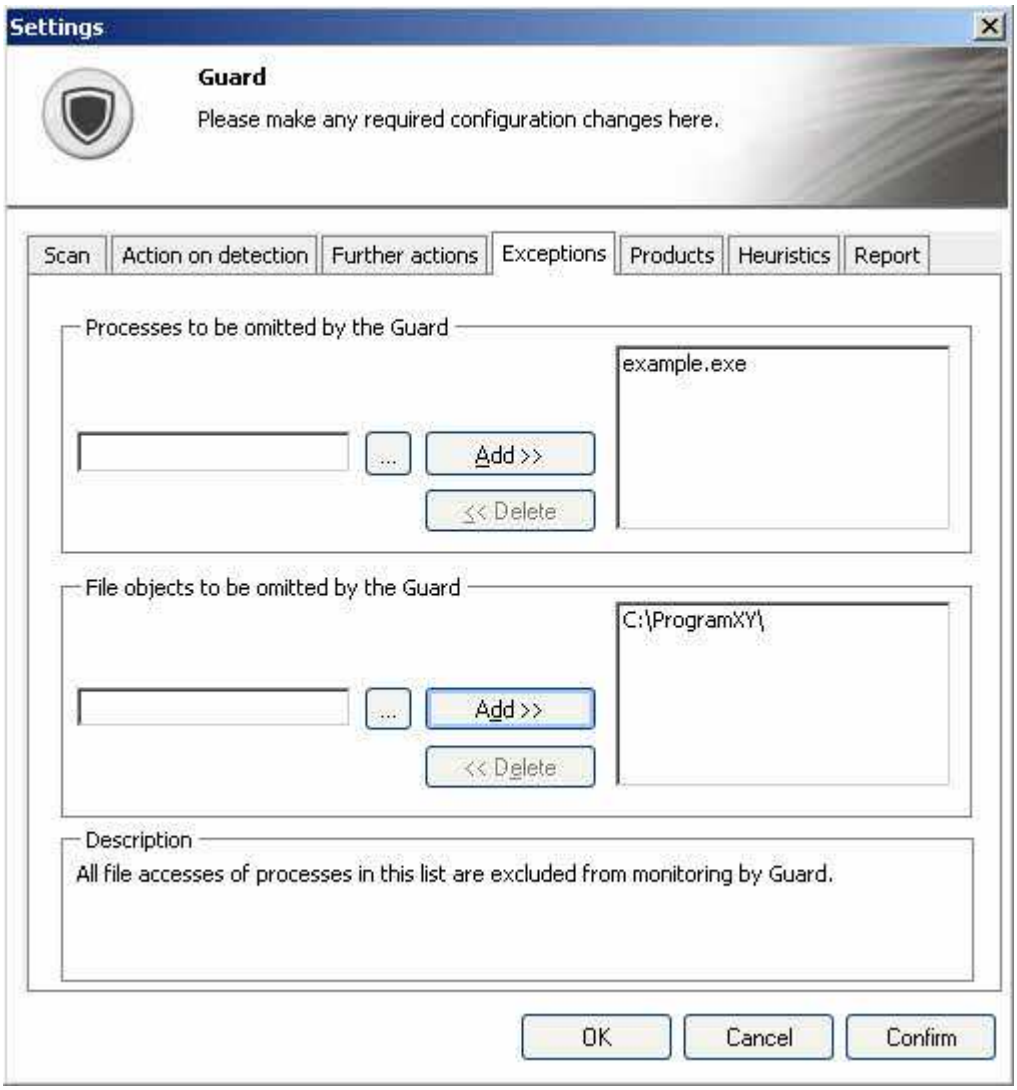
Furthermore it is important to exclude also the processes of the excluded software from the scan.

These running processes like e.g. backup software initialize accesses to files. In case the process itself is not excluded, the guard scans every read access.

So find out which processes the software uses by means of the task manager and enter them into the box “Processes to be skipped by the guard”.

An active process, e.g. of a backup program needs read and write accesses to the hard disk. The guard would scan all these accesses if the process is not excluded

from the scan. In case only the program directory is omitted by the guard scan the guard will not be active in this directory. But this doesn't concern all active processes in the task manager.




It is also important for the execution of the scan to exclude the program folders of the corresponding software from the scanner. This can be done in the menu "Scanner" → "Scan" → "Exception".

## 3. Jobs in the scheduler

The Avira AntiVir Server offers an integrated scheduler for one-time or regular jobs, like e.g. updates and scans.
You should enter the settings for this scheduler after the installation, so that updates and scans are proceeded automatically.

Start the Avira AntiVir Server GUI and choose the point “Scheduler”. Click in the task bar on “Create new job using wizard”. Define a name (e.g. internet update or weekly scan) and a short description for the job.
Choose the kind of job (in case of an update choose “Update job”, in case of a scan choose scan job).

In case of a scan job you can choose the profile which should be used for the scan. You find further information about the scan profiles in chapter 4 of this document.

Configure afterwards when the job should be executed. (e.g. immediately, daily, interval, single).

Please, check if the job is shown as “Ready” in the overview.

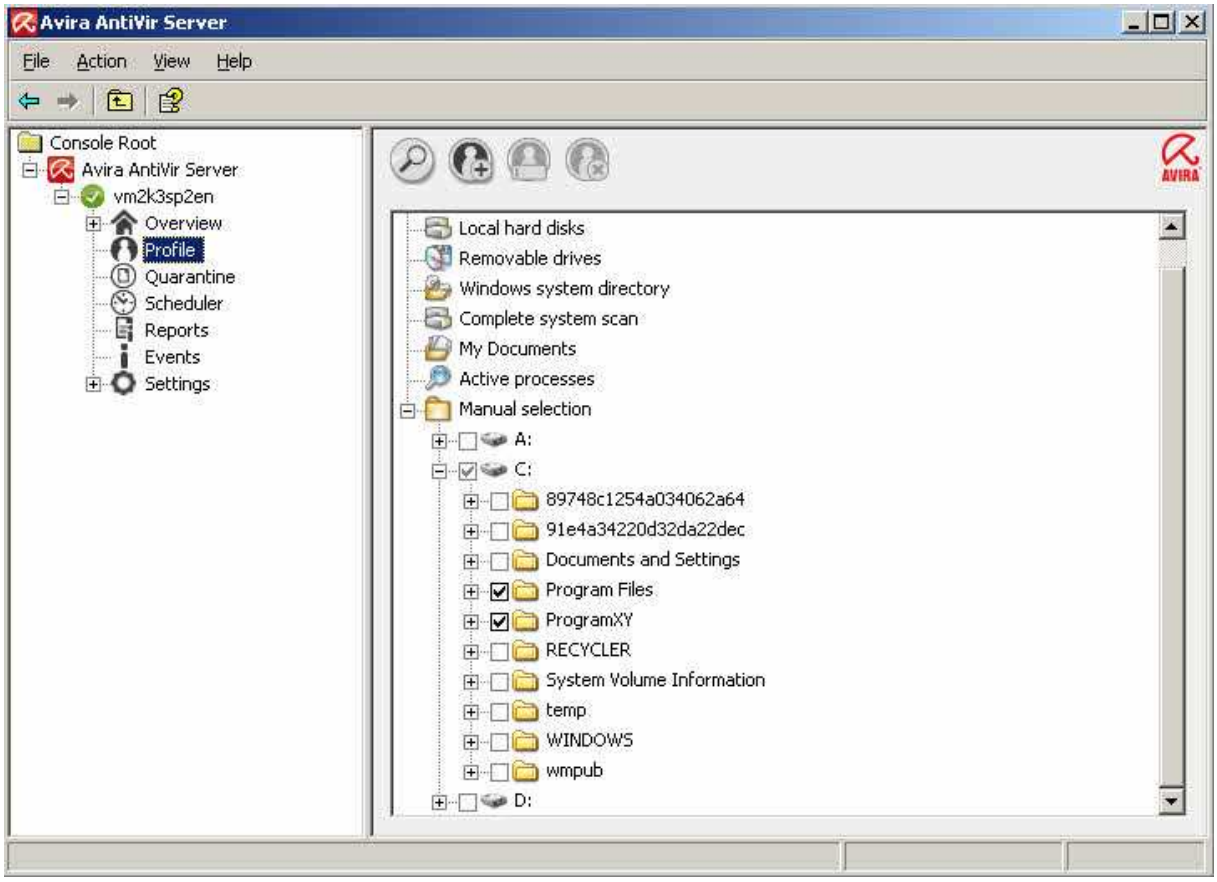
**We recommend you an hourly update and a weekly scan.**

We proceed daily about 5 updates of our virus definition files and/or the engine. With an hourly update you make sure to benefit from these security updates.
The weekly system scan is also important for your security. Very frequent system scans could cause a loss of performance. Large time periods without scans might increase the risk of viruses on the PC which could be detected after the scan.
If you make an update after a gap of several weeks or months, AntiVir can detect a virus which might have already been active for a certain time on the server in case the AntiVir Guard hasn’t already found it.
Therefore a weekly system scan is a good balance between low system load and an optimum of security of the system.

## 4. Different scan profiles

In case of a possible virus attack or a general control, AntiVir offers predefined scan profiles and the possibility to create individual scan profiles. By means of these profiles you can make the virus scan more effectively, so that only special sectors, drives or directories of the system are scanned.
In the following, we give you an overview of the predefined scan profiles and the possibility to adapt the scan to your individual demands.

You can find the profiles for the scan in the menu “Profile” beneath in the control menu of Avira AntiVir Server.




Which scan profile is the best depends on which data have to be checked or excluded from the scan.

In case of a virus attack which can be localized on the local drives, the profile “Local drives” shortens the scan considerably. The profile “Local drives” also scans cd drives and removable media.

New unknown USB sticks which are connected to the PC should also be checked. As a complete system scan is not necessary, you can use the profile “Removable Drives” in order to make sure that there are no viruses on removable media.

In case of a virus attack, you can check if a virus is already running. The scan profile “Active Processes” looks for processes that are being processed.

The following list shows an overview of the predefined profiles and different scenarios when they should be used:

| Scan profile | Explanation | Scenario |
|---|---|---|
| Local Drives | This profile checks all local drives. | In case you don't know on which drive a virus is. |
| Local Hard Disk | This profile only checks the local hard disk on your system. | If you are sure that the virus is on the local hard disks and not on removable drives and you want to check the local hard disk directly. |
| Removable Drives | This profile checks all available removable drives. | If you want to make sure that a removable drive is not virulent. |
| Windows System Directory | Checks only the system directory of Windows (C:\Windows\System32) | If you want to make sure that the system files of Windows are clean. Many viruses write themselves into the system directory. This is a first important check if you suspect a virus attack. |
| Complete system scan | Makes a complete check with special scan options and will be synchronized with the GUI (server overview). | In case you don't know if there is a virus attack and where it might be. |
| My Documents | Scans the folder "My Documents" of the user who is signed on. | Windows saves downloads and similar files into "My Documents" Therefore you can look here for viruses first. |
| Active Processes | Scans all running processes. | Check if there is a virus among the running processes. |

In order to adjust the scan for special drives and directories you can use the default profile "Manual Selection" or you can create individual scan profiles.

## 5. Quarantine

If a virus or a suspicious file is found during a scan the file is moved to the quarantine depending on the setting. The file is packed into the especially encrypted format (*.qua) and moved to the quarantine directory INFECTED on your hard disk, so that no direct access is possible any more.

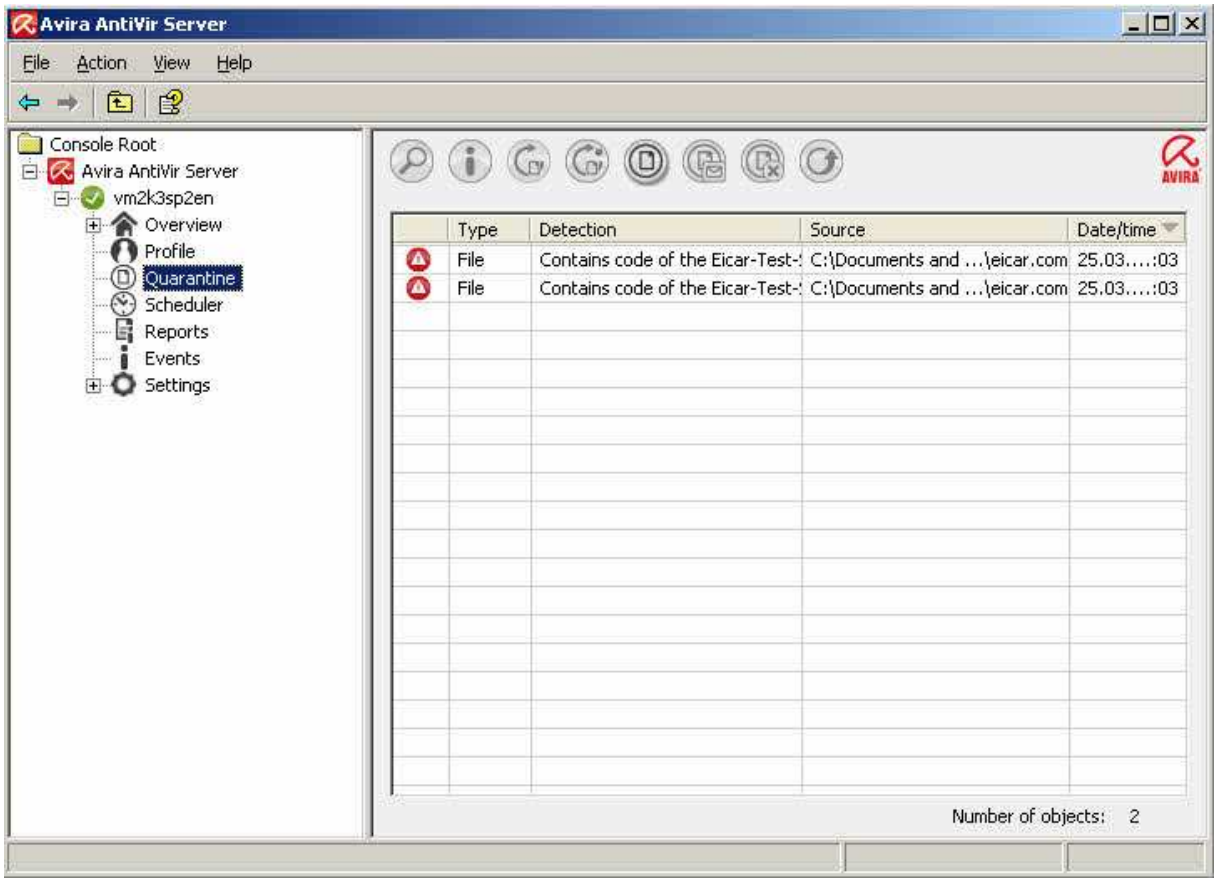
This directory is located by default in case of Windows 2000/2003 server beneath:

C:\Documents and Settings\All Users\Application Data\Avira\AntiVir Server\infected

In case of Windows Server 2008 it is located here:
C:\ProgramData\Avira\AntiVir Server\INFECTED

The files in this directory can be repaired later in the quarantine manger or they can be sent to the Avira Malware Research Center, if necessary.

You can get to the quarantine administration of the AntiVir Srever by starting the AntiVir Server gui and choosing the point “Quarantine”.




**Tip:**
In the following cases, we recommend an analysis by the Avira Malware Research Center:

**Heuristic Detection (suspicious files):** A scan has detected a suspicious file. It has been moved to the quarantine. In the Windows dialogue of the virus detection or in the report file an analysis of the file by the Avira Malware Center has been recommended.

In case of heuristic detections the name of the detected file begins with “HEUR/…” in order to show a detection of the Advanced Heuristic Analysis and Detection (AHeAD) or ends with “.gen” if it is a generic file.
A generic detection routine is used in order to detect common characteristics of different variants.
The generic detection routine has been developed in order to detect unknown variants of already known viruses and is advanced continuously.
In case of a heuristic detection of the AHeAD the file is suspicious because of its behavior. It is possible that the file is not a virus but it might be a new unknown virus. Therefore the files should be sent to Avira for analysis.

**Suspicious file:** You think a file is suspicious and you moved it to the quarantine. But the check of the file for viruses and malware is negative.

**False positive:** You are quite sure that a detection is a false positive: Avira AntiVir Professional detects a file which is very unlikely to be malware.

**Tip**
The size of the file is limited to 20 MB unpacked or 8 MB packed.
You can upload several files by marking all files you want to upload and by clicking on the button “Send object”.

You should also scan the suspicious files after a few days (between 5 and 10) with the latest virus definitions (press “F2” or right click and “Rescan object”). If the files are detected again they are very likely to be real viruses and should be deleted. If they are not detected as malware they have been false positives and can be restored.

## 6. Quick Tips

### Procedure in case of a virus attack

If the guard or the scanner should detect a virus on your system, you should scan the whole system for infected files. As many programs have exclusive read and write access on different files, a scan in the safe mode is reasonable.
As the safe mode is not available on server operation systems we recommend you to boot with our rescue CD and to clean the PC with this CD in case of a definitive attack.
You find the rescue CD on the following link:

http://www.avira.de/en/support/support_downloads.html

### Manual insertion of the license file

After renewing the license you can copy the license file (hbedv.key) directly into the main directory of AntiVir. (C:\Program Files\Avira\AntiVir Server).
You can also enter the license file in the server console by clicking on AntiVir Server with the right mouse button and choosing the point “Update license file”.

## Keeping the configuration for several installations

You can install the Avira AntiVir Server on several PCs and use a defined configuration on all the PCs by means of the “avnetnt.ini”. You can find it in the following path:

Windows Server 2003:
C:\ Documents und Settings\All Users\Application Data\Avira\AntiVir Server\config\avnetnt.ini

Windows Server 2008:
C:\Programm Data\Avira\AntiVir Server\config\avnetnt.ini

You can copy this file afterwards from one PC to another and set the configuration (it is necessary to deactivate the process protection and the Avira services).
Or you enter the path to the avnetnt.ini via the command line during the installation e.g. in case of a logon script. The avwin.ini is imported during the installation.
You find more detailed information about that in the AntiVir Server manual in the chapter “Command line parameters for the setup program”.

## Extended threat categories

**Dialer programs for chargeable numbers (Dialers)**
Installed on a computer these programs – shortly called dialers – guarantee the connection via a corresponding premium rate number whose pricing can be very different.
Some dialers replace the default EDI connection from the Internet user to the ISP (Internet service provider) and call for each connection a chargeable and usually very expensive 0190/0900 number.

**Games**
Research has shown that the working time used for computer games has reached an economically significant dimension. Therefore, more and more businesses want to keep workstations clear of games.

**Jokes**
Joke programs only want to scare or amuse people without being really dangerous. But be careful! Characteristics of joke programs can also originate from a virus or Trojan.

**Security Privacy Risk (SPR)**
Software which endangers the security of your system, doesn’t proceed the desired program activities, invades your privacy or spies out your user behaviour and is therefore not wanted.

**Back-door client (BDC)**
In order to steal data or manipulate computers, a back-door server program is locked in via the “back-door” so that the user doesn’t become aware of it. This program can be controlled by a back-door control software via the Internet or network.

**Adware/Spyware**
Software that displays advertising or sends the user’s personal data to a third party is usually unwanted.

**Unusual runtime compression**
Files which have been compressed using unusual run-time compression can be regarded as suspicious.

**Double-extension files**
Executable files which hide their real extensions in a suspicious way can be malware.

**Phishing**
Phishing also known as brand spoofing, is a clever kind of data theft which targets customers or potential customers of Internet service providers, banks, online banking services and registry authorities. By entering the email address into the Internet, in an online form or in a newsgroup or website you enable so-called “Internet crawling spiders” to steal your data which is used afterwards for a fraud or other crimes.

**Application (APPL)**
This is an application which may pose a risk for the user and has a suspicious background. Avira AntiVir Professional detects “Application (APPL)”. If you have chosen this option in the extended threat categories you receive a warning if Avira AntiVir Professional detects such a behavior.